

Préservation of integrity of program generating confidential data for access to confidential information or services

Patent Number: FR2796175
Publication date: 2001-01-12
Inventor(s): CHABANNE HERVE
Applicant(s): SAGEM (FR)
Requested Patent: ☐ FR2796175
Application Number: FR19990008937 19990709
Priority Number(s): FR19990008937 19990709
IPC Classification: G06F12/14; H04L9/32
EC Classification: G06F1/00N1D1, G06F12/14B, G06F21/00N1C6, G06F21/00N1D1
Equivalents:

Abstract

The program operates with a user key to generate a key to access sensitive data encrypted with a random key. The random key is encrypted with access key. The validity of the user key is tested. The system is implemented on a smart card with non-volatile memory for the sensitive data (22) and program (23), a processor (20,30,32) and volatile memory (26) for other data.

Data supplied from the esp@cenet database - I2

BEST AVAILABLE COPY

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 09.07.99.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 12.01.01 Bulletin 01/02.

⑤6 Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

⑥0 Références à d'autres documents nationaux
apparentés :

⑦1 Demandeur(s) : SAGEM SA Société anonyme — FR.

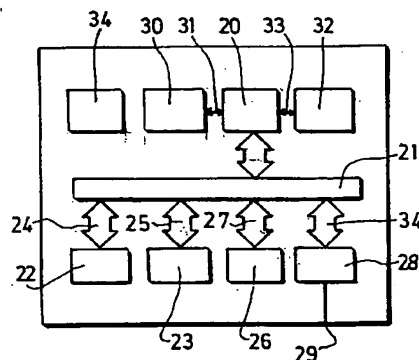
⑦2 Inventeur(s) : CHABANNE HERVE.

⑦3 Titulaire(s) :

⑦4 Mandataire(s) : CABINET BLOCH.

⑤4 PROCÉDE DE PRESERVATION DE L'INTEGRITE DE DONNEES LOGICIEL DE MISE EN OEUVRE DE
DONNEES SENSIBLES CONFIDENTIELLES ET CARTE SUPPORT DE CES DONNEES.

⑤7 Dans le procédé de l'invention, on dérive des données
logiciel (6) et d'un code porteur (1), une clé (9) d'accès à ces
données sensibles (7) qu'on crypte par une clé aléatoire
(11) et on crypte la clé aléatoire par la clé d'accès (9). Le
procédé est mis en oeuvre à l'aide d'une carte support de
données, qui comprend des mémoires non volatiles (22, 23)
de stockage des données sensibles cryptées (22), des don-
nées logiciel (23) et de données d'adressage cryptées (22),
une unité de calcul (20, 30, 32) et des mémoires volatiles
(26) de stockage des données autres que celles stockées
dans les mémoires non volatiles.



FR 2 796 175 - A1



Procédé de préservation de l'intégrité de données logiciel de mise en oeuvre de données sensibles confidentielles et carte support de ces données

5

Le domaine technique de l'invention est celui de l'embrouillage, ou du cryptage, ou du chiffrement de données sensibles, quel que soit le domaine économique d'application. Dans le domaine technique considéré, les clés de chiffrement elles-mêmes constituent des données sensibles
10 mais il y en a plein d'autres comme, par exemple, des états de compte, dans le cas d'applications bancaires, des contenus d'agendas téléphoniques et d'agendas de rendez-vous, des données d'exploitation de programmes ainsi que des codes porteurs, c'est-à-dire des codes d'utilisation de cartes supports de ces données sensibles dans lesquels
15 elles sont stockées. Il peut s'agir de cartes à micro-circuit, dites à puce, à alimentation externe, ou de cartes PCMCIA, plus épaisses, à alimentation intégrée possible.

Ces données sensibles sont mises en oeuvre par des données logiciel, c'est-à-dire, et par exemple, des programmes de mise en oeuvre et, par
20 exemple encore, des programmes de consultation des agendas.

Deux contraintes doivent être respectées :

25 1) préserver l'intégrité des données logiciel,

2) préserver la confidentialité des données sensibles.

La demanderesse a déjà proposé, dans FR-A-2 758 898, un procédé de
30 préservation de l'intégrité des données logiciels.

La présente demande vise, d'une part, à perfectionner ce procédé de préservation et, d'autre part, à proposer une mise en oeuvre appropriée dans une carte support du procédé de préservation, aussi bien d'ailleurs
35 du procédé de la présente demande que du procédé de l'art antérieur évoqué précédemment.

Le document FR-A-2 758 898 enseigne de préserver l'intégrité de données logiciel de mise en oeuvre de données sensibles confidentielles en dérivant de ces données logiciel et d'un code porteur, une clé (d'accès) pour crypter les données sensibles puis en cryptant ces données sensibles par cette clé d'accès.

De surcroît, et pour accéder à ces données sensibles, qui sont stockées cryptées dans une carte support, il faut que le porteur de la carte saisisse tout d'abord le code porteur associé à la carte.

1) Procédé perfectionné de préservation de l'intégrité des données logiciel

La présente demande concerne donc tout d'abord un procédé de préservation de l'intégrité de données logiciel de mise en oeuvre de données sensibles confidentielles, dans lequel on dérive, de ces données logiciel et d'un code porteur, une clé d'accès à ces données sensibles, caractérisé par le fait qu'on crypte les données sensibles par une clé aléatoire et qu'on crypte la clé aléatoire par la clé d'accès.

Ainsi, pour décrypter les données sensibles, il faut préalablement saisir le bon code porteur et ne pas avoir modifié les données logiciel. Si l'un ou l'autre a subi une altération, la clé aléatoire cryptée ne peut pas être décryptée pour décrypter les données sensibles.

L'avantage du procédé de l'invention, par rapport à celui de l'art antérieur, réside dans le fait que, si l'utilisateur change son code porteur, il n'est pas nécessaire de recrypter les données sensibles, il suffit de recrypter la clé aléatoire.

2) Carte support pour la mise en oeuvre du procédé

La présente demande concerne aussi une carte support de données, dont

- des données sensibles confidentielles cryptées,
- des données logiciel de mise en oeuvre des données sensibles,

- des données d'adressage cryptées,
comprenant des moyens mémoires non volatiles de stockage des données
sensibles cryptées, des données logiciel et des données d'adressage
cryptées,

5 une unité de calcul de cryptage et de décryptage et des moyens mémoires
volatiles associés à l'unité de calcul et de stockage des données autres que
celles stockées dans les moyens mémoires non volatiles.

10 Ainsi, les adresses en clair et les données sensibles en clair, après qu'elles
aient été décryptées, ne sont présentes que dans des moyens mémoires
volatiles. En cas de coupure d'alimentation d'une carte à puce, pour
reprendre cet exemple, les données stockées dans les moyens mémoires
volatiles sont effacées, contrairement aux autres. A titre d'exemple, après
15 avoir fait usage de sa carte, l'usager la retire de l'appareil d'exploitation
et le retrait de la carte provoque une opération de reset qui efface les
moyens mémoires volatiles : plus aucune donnée sensible en clair ne se
trouve dans la carte. En cas de vol, le dommage n'est pas trop excessif.
Dans les moyens mémoires non volatiles, les données sensibles sont
cryptées et si le voleur ne connaît pas le code porteur, ou si ce code n'a
20 pas encore été saisi, le voleur ne peut pas exploiter la carte.

Comme mémoires volatiles, on utilisera aujourd'hui des mémoires RAM,
comme mémoires non volatiles, des mémoires E²PROM, ROM ou
FLASH.

25

L'invention sera mieux comprise à l'aide de la description suivante des
organigrammes des processus 1) de cryptage et stockage de données
sensibles cryptées confidentielles et 2) de décryptage de ces données
sensibles cryptées ainsi que de la carte support et de stockage de ces
30 données sensibles confidentielles cryptées, en référence aux
représentations en annexe de ces organigrammes et du schéma bloc de la
carte support.

1) Processus de cryptage (figure 1)

35

On soumet un code porteur 1 à une première fonction cryptographique 2 pour obtenir une clé usager KUSR3. Cette première fonction est ici de type condensation. Parallèlement, on crypte 4, sous la clé KUSR, les adresses 5, d'une mémoire, de données logiciel 6 de mise en oeuvre de données sensibles confidentielles 7.

On soumet, à une deuxième fonction cryptographique 8, la clé KUSR, d'une part, et les données logiciel 6 et leur adresses 5 pour en tirer une clé 9, dite clé d'accès, qui servira au décryptage ultérieur.

On crypte 10, sous une clé aléatoire KDM 11, les données sensibles 7 pour obtenir les données sensibles cryptées 12.

Parallèlement, on crypte 13, sous la clé d'accès 9, la clé KDM pour obtenir la clé KDM cryptée 14.

2) Processus de décryptage (figure 2)

Au code porteur 1, saisi sur un clavier, on tire, à l'aide de la première fonction de cryptage 2, la clé KUSR 3. A l'aide de cette clé KUSR, on décrypte 4' les adresses cryptées 15 des données logiciel 6 de mise en oeuvre des données sensibles confidentielles 7.

On soumet les données logiciel 6, associées aux adresses en clair 5, et la clé KUSR à la deuxième fonction de cryptage 8 pour en tirer la clé d'accès 9.

On décrypte 13' la clé aléatoire KDM cryptée 14 pour en tirer cette clé aléatoire 11, puis on décrypte 10' les données sensibles cryptées 12 à l'aide de la clé DKM pour en tirer les données sensibles 7.

En réalité, on tire du code porteur, saisi dans la carte sur un clavier, une clé, qui devrait être KUSR, mais qui pourrait être KUSR'. Après avoir décrypté KDM cryptée 14 sous KUSR', on obtient une clé KDM'. Puis sous KDM', on tire KUSR" de KUSR. On procède enfin au test de

l'identité de KUSR' et KUSR" et ce n'est que si le test est positif que le code porteur est validé.

3) Carte support (figure 3)

5

Il s'agit ici d'une carte à micro circuit organisée autour d'unité centrale à microprocesseur 20. A l'unité 20 sont associés

- un bus principal 21,
- un groupe de mémoires non volatiles, en l'espèce une mémoire E²PROM réinscriptible 22 et une mémoire ROM non réinscriptible 23, par des bus 24 et 25 respectivement et le bus 21,
- des moyens mémoires volatiles, en l'espèce une mémoire réinscriptible RAM 26, par un bus 27 et le bus 21,
- une interface entrée/sortie 28 reliée au bus 21, par un bus 34, et à un port d'accès 29 de la carte,
- une unité arithmétique et logique de calcul 30, par un bus 31,
- une unité de calcul cryptographique 32, par un bus 33, et
- une horloge 34 reliée à tous les composants de la carte introduits ci-dessus.

20

La mémoire ROM non volatile et non réinscriptible 23 est destinée au stockage

- des logiciels 6 de mise en oeuvre des données sensibles,
- des programmes de calcul de cryptage et de décryptage,
- des fonctions cryptographiques.

25

La mémoire E²PROM non volatile et réinscriptible 22 est destinée au stockage

- des données sensibles cryptées 12,
- des adresses cryptées 15 des logiciels 6 de mise en oeuvre des données sensibles,
- de la clé aléatoire KDM cryptée 14.

30

On notera que la clé aléatoire KDM peut être générée par la carte par exemple lors de sa pré-personalisation.

35

La mémoire RAM volatile réinscriptible 26 est destinée au stockage
- du code saisi par le porteur de la carte sur un appareil d'exploitation, à travers le port 29,

- des données intermédiaires de calcul et
- 5 - des données confidentielles en clair, c'est-à-dire des données sensibles, des adresses des logiciels, de la clé d'accès, de la clé aléatoire.

On a associé à chaque ensemble de données une mémoire particulière. Naturellement, toutes ces mémoires pourraient être regroupées à volonté,
10 sous réserve de préserver, d'un côté, au moins une mémoire non volatile pour les données confidentielles cryptées, les données logiciel à préserver et toutes les données de calcul et de décryptage et, d'un autre côté, au moins une mémoire volatile pour les données en clair.

15 Lorsque la carte n'est pas activée, toutes les données sensibles sont stockées chiffrées dans la carte. Lorsque la carte est activée, les données sensibles ne sont présentes en clair qu'en mémoire volatile.

20 Lorsque le porteur de la carte change son code, une nouvelle clé KUSR est calculée et la clé KDM est transcryptée de l'ancienne clé KUSR à la nouvelle. On rappellera ici que le piratage de la carte ne peut avoir lieu que si son propriétaire légitime a saisi son code porteur.

REVENDICATIONS

1.- Procédé de préservation de l'intégrité de données logiciel (6) de mise en oeuvre de données sensibles confidentielles (7), dans lequel on dérive
5 (8), de ces données logiciel (6) et d'un code porteur (1), une clé (9) d'accès à ces données sensibles (7), caractérisé par le fait qu'on crypte les données sensibles (7) par une clé aléatoire (11) et qu'on crypte la clé aléatoire par la clé d'accès (9).

10 2.- Procédé de préservation de l'intégrité des données logiciel (7) selon la revendication 1, dans lequel on procède à un test de la validité du code porteur (1).

15 3.- Carte support de données, dont

- des données sensibles confidentielles cryptées (12),
- des données logiciel (6) de mise en oeuvre des données sensibles (7),
- des données d'adressage cryptées (15)
comprenant des moyens mémoires non volatiles (22; 23) de stockage des
20 données sensibles cryptées (22), des données logiciel (23) et des données d'adressage cryptées (22),
une unité de calcul de cryptage et de décryptage (20, 30, 32) et des moyens mémoires volatiles (26) associés à l'unité de calcul (20) et de
stockage des données autres que celles stockées dans les moyens
25 mémoires non volatiles.

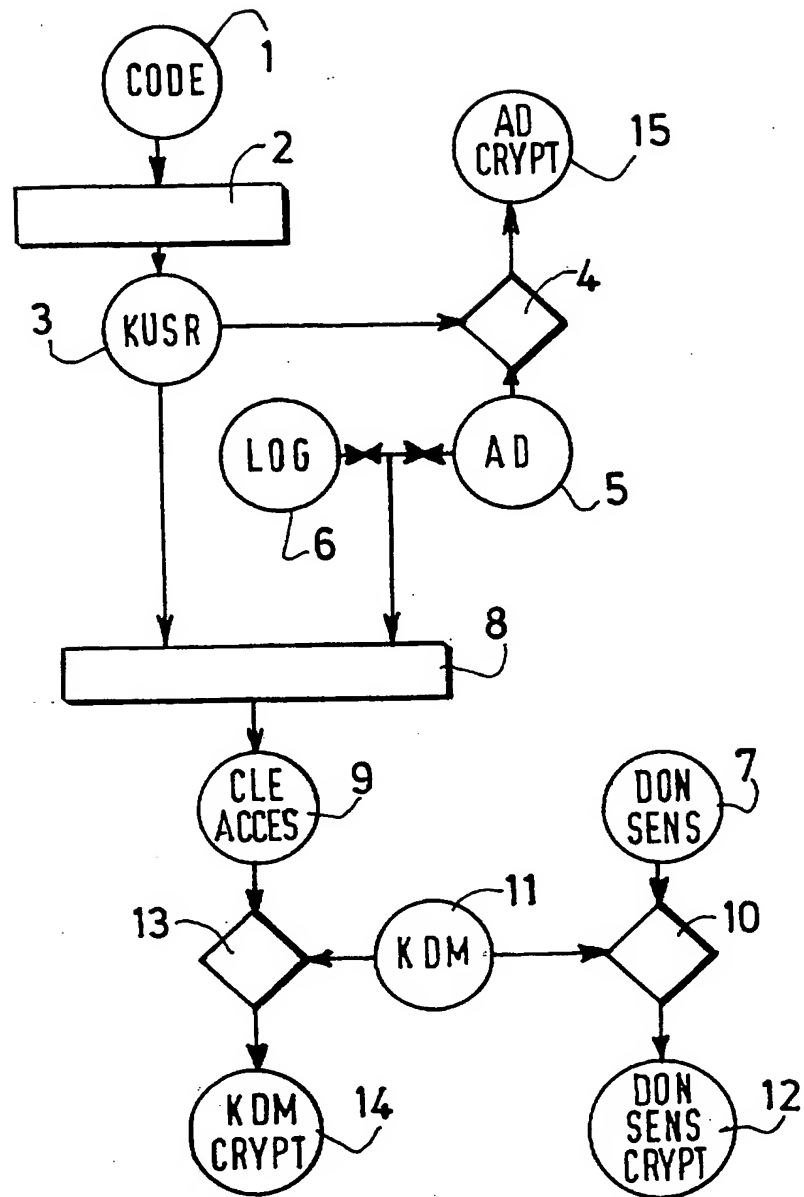
4.- Carte support selon la revendication 3, dans laquelle les mémoires non volatiles (21) comprennent une mémoire E²PROM (22) et une mémoire ROM (23).

30 5.- Carte support selon l'une des revendications 3 et 4, dans laquelle il est prévu une mémoire volatile RAM (26).

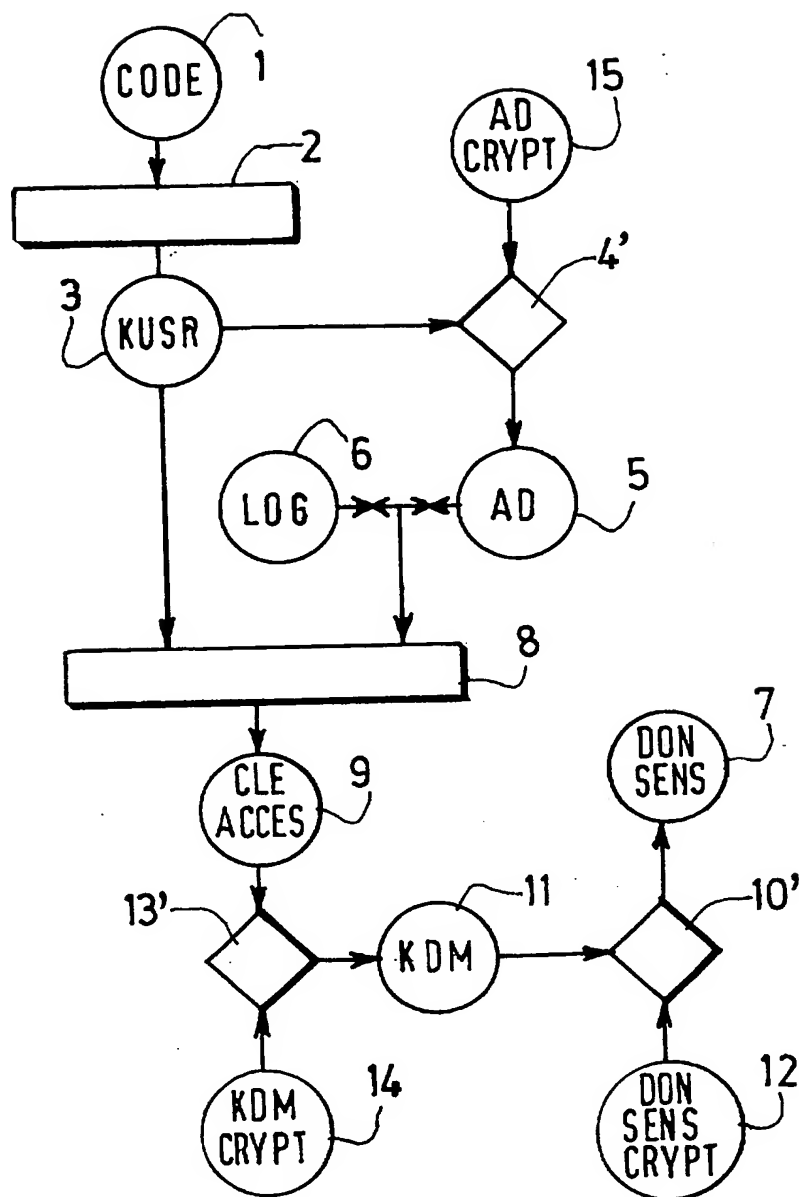
35 6.- Carte support selon l'une des revendications 3 à 5, qui est une carte à micro-circuit.

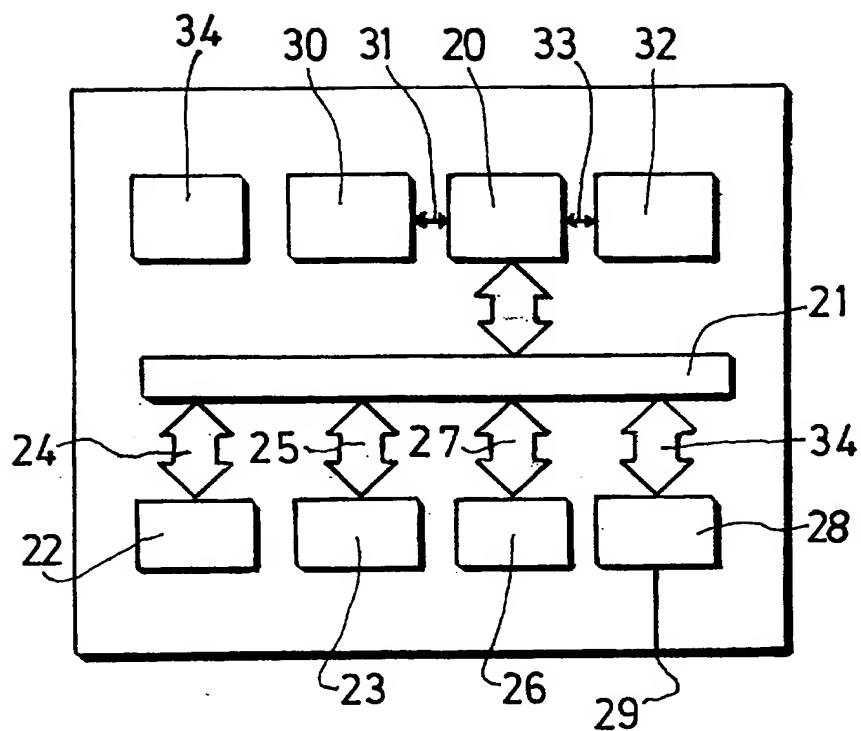
7.- Carte support selon l'une des revendications 3 à 5, qui est une carte PCMCIA. •

1/3

FIG.1

2/3

FIG.2

FIG.3

RAPPORT DE RECHERCHE
PRELIMINAIREétabli sur la base des dernières revendications
déposées avant le commencement de la rechercheN° d'enregistrement
nationalFA 579828
FR 9908937

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	US 5 623 546 A (HARDY ET AL) 22 avril 1997 (1997-04-22) * le document en entier *	1-7
A	US 5 428 685 A (Y. KADOOKA ET AL.) 27 juin 1995 (1995-06-27) * colonne 1, ligne 5 - colonne 3, ligne 36 * * colonne 4, ligne 5 - colonne 5, ligne 47; revendications; figures 1-4 *	1-7
D,A	EP 0 855 652 A (SAGEM) 29 juillet 1998 (1998-07-29) * le document en entier *	1-7
A	EP 0 867 843 A (SONY) 30 septembre 1998 (1998-09-30) * colonne 1, ligne 5 - colonne 12, ligne 45; revendications; figures 1-4 *	1
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)
		G07F G06F
Date d'achèvement de la recherche 10 mai 2000		Examineur Soler, J
CATEGORIE DES DOCUMENTS CITES X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant		

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.